



REQU: 18 JUIN 2004

OMPI PCT

# BREVET D'INVENTION

**CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION****COPIE OFFICIELLE**

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 07 MAI 2004

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

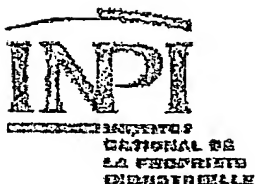
Martine PLANCHE

DOCUMENT DE PRIORITÉ  
PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17.1.a) OU b)

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint-Petersbourg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
www.inpi.fr

BEST AVAILABLE COPY



# BREVET D'INVENTION

**28 MARS 2003**  
26bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livre VI

REQUÊTE EN DÉLIVRANCE

DATE DE REMISE DES PIÈCES N° D'ENREGISTREMENT NATIONAL DÉPARTEMENT DE DÉPÔT DATE DE DÉPÔT <b>28 MARS 2003</b>	Albert GRYNWALD 127, rue du Faubourg Poissonnière 75009 PARIS France
Vos références pour ce dossier: B11023	

<b>1 NATURE DE LA DEMANDE</b>			
Demande de brevet			
<b>2 TITRE DE L'INVENTION</b>			
		PROCÉDE ET SYSTÈME DE CRYPTAGE	
<b>3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE</b>		Pays ou organisation      Date      N°	
<b>4-1 DEMANDEUR</b>			
Nom		EVERBEE NETWORKS	
Rue		41, boulevard des Capucines	
Code postal et ville		75002 PARIS	
Pays		France	
Nationalité		France	
Forme juridique		Société anonyme	
N° SIREN		432 809 663	
Code APE-NAF		721Z	
<b>5A MANDATAIRE</b>			
Nom		GRYNWALD	
Prénom		Albert	
Qualité		CPI: 95-1001	
Cabinet ou Société		Cabinet GRYNWALD	
Rue		127, rue du Faubourg Poissonnière	
Code postal et ville		75009 PARIS	
N° de téléphone		01 53 32 77 34	
N° de télécopie		01 53 32 77 94	
Courrier électronique		cabinet.grynwald@wanadoo.fr	
<b>6 DOCUMENTS ET FICHIERS JOINTS</b>		Fichier électronique      Pages      Détails	
Désignation d'inventeurs			
Description		b11023 dépôt.pdf      31	
Revendications		b11023 dépôt.pdf      17      22	
Dessins		b11023 dépôt dessins.pdf      3      3 fig., 1 ex.	
Abrégé		b11023 dépôt.pdf      1	

Listage des sequences, PDF	
Rapport de recherche	
Chèque	
<b>7 RAPPORT DE RECHERCHE</b>	
Etablissement immédiat	
<b>8 REDEVANCES JOINTES</b>	Devise      Taux      Quantité      Montant à payer
Total à acquitter	EURO                0.00
<b>9 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b>	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.  
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.



## PROCEDE ET SYSTEME DE CRYPTAGE

La sécurisation des communications par voie électronique prend une importance croissante avec le développement du réseau Internet et de ses applications. Les besoins en sécurité dépassent largement le cadre des communications professionnelles entre les entreprises et leurs clients. Plus généralement ce sont toutes les communications par courrier électronique, y compris les communications grand public, qui devraient être protégées contre la lecture, et, plus grave, contre une éventuelle modification, par un acteur non autorisé.

De nombreuses techniques de cryptage sont disponibles et permettent d'obtenir un texte crypté de même longueur que le clair et dans lequel tous les 256 octets possibles sont équiprobables, ce qui couramment considéré par les cryptologues comme une condition nécessaire. Elles peuvent être classées en deux grandes familles, les algorithmes par blocs et les algorithmes par masque.

Les algorithmes par blocs découpent le texte en blocs de longueur fixe, le cryptage ou le décryptage se faisant bloc par bloc et donnant comme résultat un bloc de même longueur que le bloc qui avait été fourni. Il en est ainsi du cryptage par le système DES - Data Encryption Standard--,-utilisant--des blocs de

8 octets, admis comme standard aux USA en 1976, et devenu depuis standard de fait mondial, ou de l'AES - Advanced Encryption Standard -, utilisant des blocs de 16 octets sélectionné en 2000 comme futur nouveau standard par les organismes officiels américains.

Les algorithmes par masque consistent à générer un masque de même longueur que le texte à crypter, et à appliquer un XOR entre le texte et le masque. Le décryptage se fait en appliquant une seconde fois un XOR avec le même masque. Ici et dans toute la suite, XOR désigne l'opération « OU EXCLUSIF, bit à bit ». On rappelle que, au niveau d'un bit, appliquer un XOR avec un bit 0 conserve le bit initial et appliquer un XOR avec un bit 1 retourne le bit initial. Le masque s'obtient par exemple par un générateur pseudo-aléatoire initialisé de la même façon des deux côtés. Le codage DES en mode OFB, standardisé depuis 1980, revient à utiliser un générateur pseudo-aléatoire particulier utilisant l'algorithme de cryptage DES.

Tous ces algorithmes fournissent des textes cryptés dans lesquels tous les octets sont équiprobables.

Malheureusement, ces algorithmes ne peuvent pas être utilisés directement pour le cryptage du courrier électronique. En effet les divers serveurs et autres dispositifs de traitement par lesquels transitent les courriers électroniques sur Internet considèrent certains octets comme des caractères de contrôle. Ces symboles peuvent alors provoquer des comportements parasites, comme par exemple le rajout systématique d'un octet x0D - retour chariot - dès que passe un octet x0A - à la ligne - non accompagné de son x0D retour chariot, ou la non prise en compte de la suite du message dès que passe un octet x00 qui est considéré comme une fin de message. N.B. : ici et dans toute la suite du texte, on note xAB l'octet contenant le nombre s'écrivant AB en codage hexadécimal. Ces perturbations rendent le message illisible et impossible à décrypter à l'arrivée.

Pour remédier à cet inconvénient, certains systèmes de cryptage du courrier électronique regroupent les bits par paquet

de 6, chacun de ces paquets étant représenté par un octet autre qu'un caractère de contrôle. Cela revient donc à transmettre 8 bits pour 6 bits utiles, et augmente donc d'un tiers le volume de données à transmettre.

5            Une autre solution peut être mise en œuvre en utilisant le codage dit ASCII à 7 bits, les symboles qui n'ont pas de code sur 7 bits - lettres accentuées, caractères spéciaux... - étant recodés sur deux symboles à 7 bits. La transmission se fait sur des octets (8 bits), dont le bit de poids fort est à 0. Si on utilise un système de cryptage par masque XOR comme décrit précédemment, on n'utilise que 7 bits du masque et on ne modifie pas le bit de poids fort qui, après application du XOR, reste à 0. Lorsque l'octet ainsi obtenu prend une valeur indésirable (x00, x0D, x0A,...) il suffit de  
10           forcer artificiellement à 1 son bit de poids fort, ce qui revient à rajouter 128 à sa valeur, avant de l'envoyer sur le réseau. L'opération de décryptage est similaire au cryptage : on applique le même masque XOR on reconstitue le texte initial après avoir forcé à 0 le bit de poids fort.

15           Cette méthode règle donc le problème des valeurs susceptibles de provoquer des phénomènes parasites indésirables. Par contre, elle nécessite, lors de la transmission, l'utilisation de 8 bits par symboles, alors que le message initial était codé sur 7 bits par symboles, d'où une  
20           augmentation d'un septième du volume de données à transmettre. Et dans certains cas, les caractères dont le bit de poids fort est à 1 peuvent provoquer d'autres effets indésirables lors de la transmission. D'une façon générale, le principal inconvénient des techniques de ce type est que le jeu de symboles utilisé par  
25           le message crypté est différent de celui utilisé pour le message en clair ce qui peut être rédhibitoire pour certaines applications. Par ailleurs l'utilisation de ces techniques reste limitée au cas du codage ASCII à 7 bits. Ces techniques ne sont donc pas compatibles avec les évolutions comme le codage ASCII 8  
30           bits ou le codage Unicode 16 bits pour prise en compte

d'alphabets non latins - cyrillique, grec, arabe, hébreux, japonais, chinois....

#### La solution selon l'invention

##### Procédé selon l'invention

5 L'invention concerne un procédé pour le cryptage et le décryptage d'une information. L'information est représentée par une suite de symboles. Les symboles sont pris dans un ensemble de symboles appelé ci-après l'alphabet.

10 Le procédé est caractérisé en ce qu'il met en œuvre un générateur pseudo-aléatoire fournissant une séquence de valeurs dénommée ci-après séquence aléatoire. Les valeurs formant la séquence aléatoire sont incluses dans un ensemble ci-après dénommé l'espace des valeurs aléatoires.

15 Le générateur pseudo-aléatoire peut être, avant utilisation et fourniture de la séquence aléatoire, initialisé au moyen d'une suite de nombres ci-après dénommée clé d'initialisation.

20 La clé d'initialisation détermine la séquence aléatoire qui sera fournie par le générateur pseudo-aléatoire, de telle sorte qu'après une initialisation ultérieure utilisant la même clé d'initialisation la séquence de valeurs fournies sera la même qu'après la première initialisation. Le générateur pseudo-aléatoire est en outre caractérisé en ce que la connaissance de la séquence des valeurs fournies ne permet pas  
25 de retrouver en un temps raisonnable la clé d'initialisation.

Le procédé comprend trois étapes préalables.

30 La première étape préalable consiste à séparer en deux parties disjointes l'alphabet, l'une des parties est ci-après dénommée l'alphabet de contrôle et est composée de symboles destinés à ne pas être modifiés lors du cryptage, l'autre partie est ci-après dénommée l'alphabet de message et est composée de symboles destinés à être éventuellement modifiés lors du cryptage. Ainsi, chacun des symboles utilisés pour représenter l'information est inclus, soit dans l'alphabet de contrôle, soit

dans l'alphabet de message, aucun symbole n'est commun à ces deux alphabets.

La deuxième étape préalable consiste à définir un ensemble, appelé alphabet de masque, formé de tout ou partie des éléments de l'espace des valeurs aléatoires.

La troisième étape préalable consiste à affecter à chaque élément de l'alphabet de masque une permutation de l'alphabet de message.

Les trois étapes préalables sont réalisées une fois pour toutes avant la première mise en œuvre du procédé.

La mise en œuvre du procédé, pour réaliser l'opération de cryptage d'une information à crypter, comprend les étapes préliminaires suivantes :

- l'étape de prendre en compte une suite de nombres ci-après dénommée la clé primaire de cryptage,
- l'étape de construire la clé d'initialisation à partir de tout ou partie de la clé primaire de cryptage.
- l'étape d'initialiser le générateur pseudo-aléatoire à l'aide de la clé d'initialisation.

Le procédé consiste à sélectionner l'un après l'autre les symboles composant l'information à crypter et à crypter chacun des symboles ainsi sélectionnés en lui appliquant les opérations suivantes :

si le symbole sélectionné appartient à l'alphabet de contrôle, il n'est pas modifié,

si le symbole sélectionné appartient à l'alphabet de message les étapes suivantes sont exécutées :

- l'étape de lire la prochaine valeur de la séquence aléatoire fournie par le générateur pseudo-aléatoire,
- si la valeur lue à l'étape précédente n'est pas un élément de l'alphabet de masque, l'étape de réitérer l'étape précédente jusqu'à obtention d'un élément de l'alphabet de masque,

l'élément de l'alphabet de masque, déterminé à l'étape précédente, sera ci-après dénommé l'élément de masque.



Les opérations comprennent également les étapes suivantes :

- l'étape de sélectionner la permutation de l'alphabet de message affectée à l'élément de masque spécifié à l'étape précédente,
- l'étape d'appliquer au symbole sélectionné la permutation de l'alphabet de message sélectionnée à l'étape précédente,
- l'étape de remplacer le symbole sélectionné par le résultat de la permutation mise en œuvre à l'étape précédente.

Ces opérations étant exécutées, on passe au symbole suivant de l'information à crypter, et ainsi de suite jusqu'à ce que tous les symboles de l'information à crypter aient été traités.

- De préférence selon l'invention, la mise en œuvre du procédé, pour réaliser l'opération de décryptage d'une information à décrypter, comprend les mêmes étapes préliminaires que lors du cryptage. Ainsi, le générateur pseudo-aléatoire sera initialisé de la même façon que lors du cryptage et fournira donc la même séquence de valeurs que lors du cryptage.

Le procédé consiste à sélectionner l'un après l'autre les symboles composant l'information à décrypter et à décrypter chacun des symboles ainsi sélectionnés en lui appliquant les opérations suivantes :

- si le symbole sélectionné appartient à l'alphabet de contrôle, il n'est pas modifié,
- si le symbole sélectionné appartient à l'alphabet de message les étapes suivantes sont exécutées :
  - l'étape de lire la prochaine valeur de la séquence aléatoire fournie par le générateur pseudo-aléatoire,
  - si la valeur lue à l'étape précédente n'est pas un élément de l'alphabet de masque, l'étape de réitérer l'étape précédente jusqu'à obtention d'un élément de l'alphabet de masque.

L'élément de l'alphabet de masque, déterminé à l'étape précédente, sera ci-après dénommé l'élément de masque.

Les opérations pour décrypter comprennent les étapes suivantes :

- 5           - l'étape de sélectionner la permutation inverse de la permutation de l'alphabet de message affectée à l'élément de masque spécifié à l'étape précédente,
- l'étape d'appliquer au symbole sélectionné la permutation inverse sélectionnée à l'étape précédente,
- 10          - l'étape de remplacer le symbole sélectionné par le résultat de la permutation mise en œuvre à l'étape précédente.

Ces opérations étant exécutées, on passe au symbole suivant de l'information à décrypter, et ainsi de suite jusqu'à ce que tous les symboles de l'information à décrypter aient été  
15 traités.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires sont des nombres, de sorte que l'alphabet de masque se compose de nombres. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet  
20 de message. La numérotation consiste à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et  $N-1$ , ci-après dénommé numéro du symbole,  $N$  représentant le nombre d'éléments de l'alphabet de message. De sorte que pour tout nombre compris entre 0 et  $N-1$  il  
25 y a un et un seul symbole de l'alphabet de message dont ce nombre est le numéro.

Dans le cas de cette variante de réalisation de l'invention, le procédé est caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de  
30 masque donné, pour un symbole donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro du symbole donné,
- l'étape d'ajouter l'élément de masque donné au  
35 numéro déterminé à l'étape précédente,

- l'étape de calculer le reste de la division par N du résultat de l'addition effectuée à l'étape précédente,

- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente, ce symbole est alors le résultat que l'on souhaitait calculer.

Il en résulte que la permutation ainsi définie correspond à une addition modulo N sur les numéros de symboles, et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée au symbole donné.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires sont des nombres, de sorte que l'alphabet de masque se compose de nombres. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet de message. La numérotation consiste à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message. De sorte que pour tout nombre compris entre 0 et N-1 il y a un et un seul symbole dont ce nombre est le numéro.

Dans le cas de cette variante de réalisation, le procédé est caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque donné, pour un symbole donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro du symbole donné,  
 - l'étape de soustraire le élément de masque donné au numéro déterminé à l'étape précédente,  
 - lorsque le résultat de la soustraction effectuée à l'étape précédente est négatif, l'étape d'ajouter à ce résultat autant de fois que nécessaire le nombre N jusqu'à obtenir un nombre positif,

- l'étape de calculer le reste de la division par N du résultat de l'étape précédente,

- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente, ce symbole est alors le résultat que l'on souhaite calculer.

5 Il en résulte que la permutation ainsi définie correspond à une soustraction modulo  $N$  sur les numéros de symboles et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée au symbole donné.

10 De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires sont des nombres, de sorte que l'alphabet de masque se compose de nombres. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet de message. La numérotation consiste à attribuer à chaque  
15 symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et  $N-1$ , ci-après dénommé numéro du symbole,  $N$  représentant le nombre d'éléments de l'alphabet de message, de sorte que pour tout nombre compris entre 0 et  $N-1$  il y ait un et un seul symbole dont ce nombre soit le numéro.

20 Dans le cas de cette variante de réalisation, l'alphabet de masque ne comprend que des nombres non nuls et premiers à  $N$ . Le procédé est caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque donné, pour un symbole donné appartenant à l'alphabet  
25 de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro du symbole donné,
- l'étape de multiplier par l'élément de masque donné le numéro déterminé à l'étape précédente,
- 30 - l'étape de calculer le reste de la division par  $N$  du résultat de la multiplication effectuée à l'étape précédente,
- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente.

Ce symbole est alors le résultat que l'on souhaitait calculer.

Il en résulte que la permutation ainsi définie correspond à une multiplication modulo  $N$  sur les numéros de symboles et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée au symbole donné.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires sont des nombres, de sorte que l'alphabet de masque se compose de nombres. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet de message. La numérotation consiste à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et  $N-1$ , ci-après dénommé numéro du symbole,  $N$  représentant le nombre d'éléments de l'alphabet de message, de sorte que pour tout nombre compris entre 0 et  $N-1$  il y ait un et un seul symbole dont ce nombre soit le numéro.

Dans le cas de cette variante de réalisation, l'alphabet de masque ne comprend que des nombres non nuls et premiers à  $N$ . Le procédé est caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque donné, pour un symbole donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro du symbole donné,
- l'étape de déterminer un nombre qui, multiplié par l'élément de masque donné, diffère du numéro déterminé à l'étape précédente, d'un multiple entier de  $N$ ,
- l'étape de calculer le reste de la division par  $N$  du nombre déterminé à l'étape précédente,
- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente.

Ce symbole est alors le résultat que l'on souhaitait calculer.

Il en résulte que la permutation ainsi définie correspond à une division modulo  $N$  sur les numéros de symboles et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée au symbole donné.

5 De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires sont des nombres, de sorte que l'alphabet de masque se compose de nombres. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet de message. La numérotation consiste à attribuer à chaque  
10 symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et  $N-1$ , ci-après dénommé numéro du symbole,  $N$  représentant le nombre d'éléments de l'alphabet de message de sorte que pour tout nombre compris entre 0 et  $N-1$  il y ait un et un seul symbole dont ce nombre soit le numéro.

15 L'alphabet de masque ne comprend que des nombres non nuls et premiers à  $\Phi(N)$  où  $\Phi(N)$  désigne le nombre d'entiers compris entre 1 et  $N-1$  et premiers à  $N$ .

Dans le cas de cette variante de réalisation, le procédé est caractérisé en ce que le résultat de la permutation  
20 de l'alphabet de message associée à un élément de masque donné, pour un symbole donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro du symbole donné,
- l'étape de calculer le reste de la division par  $N$   
25 du résultat de l'élévation du numéro déterminé à l'étape précédente à une puissance égale à l'élément de masque donné,
- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente.

30 Ce symbole est alors le résultat que l'on souhaitait calculer. De sorte que la permutation ainsi définie correspond à une exponentiation modulaire sur les numéros de symboles et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée audit symbole donné.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires sont des nombres, de sorte que l'alphabet de masque se compose de nombres. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet de message. La numérotation consiste à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et  $N-1$ , ci-après dénommé numéro du symbole,  $N$  représentant le nombre d'éléments de l'alphabet de message, de sorte que pour tout nombre compris entre 0 et  $N-1$  il y ait un et un seul symbole dont ce nombre soit le numéro.

L'alphabet de masque ne comprend que des nombres non nuls et premiers à  $\Phi(N)$  où  $\Phi(N)$  désigne le nombre d'entiers compris entre 1 et  $N-1$  et premiers à  $N$ .

Dans le cas de cette variante de réalisation, le procédé est caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque donné, pour un symbole donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro du symbole donné,
- l'étape de déterminer un nombre positif, qui, élevé à une puissance égale à l'élément de masque donné, diffère du numéro déterminé à l'étape précédente d'un multiple entier de  $N$ ,
- l'étape de déterminer le reste de la division par  $N$  du nombre déterminé à l'étape précédente,
- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente.

Ce symbole est alors le résultat que l'on souhaitait calculer. Il en résulte que la permutation ainsi définie correspond à l'extraction d'une racine en arithmétique modulaire sur les numéros de symboles et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée au symbole donné.

De préférence selon l'invention, le procédé comprend une opération préalable consistant à associer à chaque élément

de l'alphabet de masque un quadruplet de nombres notés  $p$ ,  $q$ ,  $r$  et  $s$  et tels que le nombre  $r$  et le résultat de l'expression  $p.s-q.r$  soient tous deux des nombres non nuls et non multiples de  $N$ ,  $N$  représentant le nombre d'éléments de l'alphabet de message. Le procédé comprend en outre une opération préalable de numérotation de l'alphabet de message, la numérotation consistant à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et  $N-1$ , ci-après dénommé numéro du symbole, de sorte que pour tout nombre compris entre 0 et  $N-1$  il y ait un et un seul symbole dont ce nombre soit le numéro.

Dans le cas de cette variante de réalisation, le procédé est caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque donné, pour un symbole donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le quadruplet de nombres  $p$ ,  $q$ ,  $r$  et  $s$  associé à l'élément de masque donné,
- l'étape de déterminer le numéro du symbole à crypter ou à décrypter, ce numéro est ci-après noté  $m$ ,
- l'étape de calculer l'expression  $m.r + s$ ,
- l'étape, lorsque le résultat du calcul effectué à l'étape précédente est nul ou est un multiple de  $N$ , de calculer un nombre  $k$  tel que l'expression  $k.r - p$  soit un multiple de  $N$ ,
- l'étape, lorsque le résultat du calcul effectué à l'étape précédente n'est ni zéro ni un multiple de  $N$ , de calculer un nombre positif  $k$  tel que l'expression  $k.(m.r + s) - (m.p + q)$  soit un multiple de  $N$ ,
- l'étape de calculer le reste de la division par  $N$  du nombre  $k$  calculé à l'étape précédente,
- l'étape de déterminer le symbole de l'alphabet de masque dont le numéro est le nombre calculé à l'étape précédente.



Ce symbole est alors le résultat que l'on souhaitait calculer. Il en résulte que la permutation ainsi définie correspond au calcul d'une fonction homographique en arithmétique modulaire sur les numéros de symboles et que le  
 5 symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée au symbole donné.

De préférence selon l'invention, le procédé met en œuvre un premier générateur pseudo-aléatoire pouvant être initialisé à l'aide de la clé d'initialisation. Les valeurs  
 10 fournies par le premier générateur pseudo-aléatoire sont utilisées comme données en entrée d'un algorithme de hachage dont les résultats sont utilisés pour fournir la séquence aléatoire. Le générateur pseudo-aléatoire consiste en la composition du premier générateur pseudo-aléatoire et de  
 15 l'algorithme de hachage.

De préférence selon l'invention, le procédé comprend en outre l'étape préliminaire de construire à partir de tout ou partie de la clé primaire de cryptage une suite de nombres appelée ci-après clé secondaire de cryptage. Le procédé met en  
 20 œuvre un premier générateur pseudo-aléatoire qui peut être initialisé à l'aide de la clé d'initialisation. Les valeurs fournies par le premier générateur pseudo-aléatoire sont cryptées à l'aide d'un premier algorithme de cryptage utilisant comme clé de cryptage la clé secondaire de cryptage. Les  
 25 résultats du premier algorithme de cryptage sont utilisés pour fournir la séquence aléatoire.

Le générateur pseudo-aléatoire consiste en la composition du premier générateur pseudo-aléatoire et du premier algorithme de cryptage.

### 30      **Système selon l'invention**

L'invention concerne également un système pour le cryptage et le décryptage d'une information. L'information est représentée par une suite de symboles. Les symboles sont pris dans un ensemble de symboles appelé ci-après l'alphabet.

L'alphabet est séparé en deux parties disjointes. L'une des parties est ci-après dénommée l'alphabet de contrôle et est composée de symboles destinés à ne pas être modifiés lors du cryptage, l'autre partie est ci-après dénommée l'alphabet de message et est composée de symboles destinés à être éventuellement modifiés lors du cryptage.

Le système est plus particulièrement destiné à sécuriser les communications entre un ordinateur ci-après dénommé l'ordinateur client et un réseau formé d'un ou plusieurs autres ordinateurs, le système est intercalé entre l'ordinateur client et le réseau. De sorte que toute information circulant entre le ordinateur client et le réseau et devant être cryptée ou décryptée, passe à travers le système. Le système comprend un générateur pseudo-aléatoire fournissant une séquence de valeurs dénommée ci-après séquence aléatoire. Les valeurs formant ladite séquence aléatoire sont comprises dans un ensemble ci-après dénommé l'espace des valeurs aléatoires. Certaines de ces valeurs sont incluses dans un sous-ensemble de l'espace des valeurs aléatoires. Ce sous-ensemble est ci-après dénommé alphabet de masque.

Le générateur pseudo-aléatoire peut être, avant utilisation et fourniture de la séquence de valeurs, initialisé au moyen d'une suite de nombres ci-après dénommée clé d'initialisation. La clé d'initialisation détermine la séquence aléatoire qui sera fournie par le générateur.

Le système comprend en outre :

- deux unités d'entrée sortie, l'une d'entre elles étant destinée à assurer les communications entre le système et l'ordinateur client, l'autre d'entre elles étant destinée à assurer les communications entre ledit système et ledit réseau,
- des premiers moyens de traitement permettant de prendre en compte une suite de nombres ci-après dénommée la clé primaire de cryptage, et de construire la clé d'initialisation à partir de tout ou partie de la clé primaire de cryptage,

- des seconds moyens de traitement permettant de décider si une valeur appartenant à l'espace de valeurs aléatoires appartient à l'alphabet de masque,

5       - des troisièmes moyens de traitement permettant de lire les valeurs successives fournies par le générateur pseudo-aléatoire, jusqu'à obtenir un élément appartenant à l'alphabet de masque,

10       - des quatrièmes moyens de traitement permettant de décider, parmi les symboles transitant à travers ledit système, quels sont les symboles qui doivent être cryptés ou décryptés et quels sont les symboles qui doivent être transmis sans modification,

- des cinquièmes moyens de traitement.

15       Ces cinquièmes moyens de traitement permettent d'une part, à partir d'un élément donné de l'alphabet de masque, ci-après appelé l'élément de masque, de sélectionner une permutation de l'alphabet de message. Cette permutation est ci-après appelée permutation affectée à l'élément de masque.

20       Ces cinquièmes moyens de traitement permettent d'autre part, la permutation affectée à l'élément de masque étant ainsi sélectionnée, et un élément donné de l'alphabet de message étant fourni par l'une des deux unités d'entrée sortie, de déterminer le résultat de cette permutation appliquée audit élément donné fourni, et d'envoyer sur l'autre des deux dites unités d'entrée  
25       sortie le résultat ainsi déterminé.

De préférence selon l'invention, les cinquièmes moyens de traitement permettant en outre de sélectionner la permutation inverse de la permutation affectée à un élément de l'alphabet de masque.

30       De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires étant des nombres, les cinquièmes moyens de traitement permettent en outre d'associer un nombre à un symbole de l'alphabet de message, de faire une addition en arithmétique modulaire entre le nombre et un élément

de l'alphabet de masque, et d'associer au résultat de cette addition un élément de l'alphabet de message.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires étant des nombres, les  
5 cinquièmes moyens de traitement permettent en outre d'associer un nombre à un symbole de l'alphabet de message, de faire une soustraction en arithmétique modulaire entre le nombre et un élément de l'alphabet de masque, et d'associer au résultat de cette soustraction un élément de l'alphabet de message.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires étant des nombres, les  
10 cinquièmes moyens de traitement permettent en outre d'associer un nombre à un symbole de l'alphabet de message, de faire une multiplication en arithmétique modulaire entre le nombre et un  
15 élément de l'alphabet de masque, et d'associer au résultat de cette multiplication un élément de l'alphabet de message.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires étant des nombres, les  
20 cinquièmes moyens de traitement permettent en outre d'associer un nombre à un symbole de l'alphabet de message, de faire une division en arithmétique modulaire entre le nombre et un élément de l'alphabet de masque, et d'associer au résultat de cette division un élément de l'alphabet de message.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires étant des nombres, les  
25 cinquièmes moyens de traitement permettent en outre d'associer un nombre à un symbole de l'alphabet de message, de faire une exponentiation en arithmétique modulaire du nombre avec pour exposant un élément de l'alphabet de masque, et d'associer au  
30 résultat de cette exponentiation un élément de l'alphabet de message.

De préférence selon l'invention, les valeurs de l'espace des valeurs aléatoires étant des nombres, les  
35 cinquièmes moyens de traitement permettent en outre d'associer un nombre à un symbole de l'alphabet de message, de faire une

extraction de racine en arithmétique modulaire, et d'associer au résultat de cette extraction de racine un élément de l'alphabet de message.

De préférence selon l'invention, le nombre de symboles composant l'alphabet de message étant ci-après dénommé  $N$ , le système comporte en outre des sixièmes moyens de traitement permettant d'associer à un élément de l'alphabet de masque un quadruplet de nombres notés  $p$ ,  $q$ ,  $r$  et  $s$ . Les cinquièmes moyens de traitement permettent en outre :

- 10           - d'associer à un symbole de l'alphabet de message, un nombre compris entre 0 et  $N-1$ , ce nombre est ci-après noté  $m$ ,
- de calculer l'expression  $m.r + s$ ,
- de déterminer si l'expression  $m.r + s$  est nulle ou multiple de  $N$ ,
- 15           - de calculer un nombre  $k$  compris entre 0 et  $N-1$  et tel que l'expression  $k.r - p$  soit un multiple de  $N$ ,
- de calculer un nombre  $k$  compris entre 0 et  $N-1$  et tel que l'expression  $k.(m.r + s) - (m.p + q)$  soit un multiple de  $N$ ,
- 20           - d'associer à un nombre  $k$  ainsi calculé un élément de l'alphabet de message.

De préférence selon l'invention, le système comprend un premier générateur pseudo-aléatoire pouvant être initialisé à l'aide de la clé d'initialisation et des moyens de calcul permettant d'appliquer un algorithme de hachage aux valeurs fournies par le premier générateur pseudo-aléatoire. Les résultats de l'algorithme de hachage sont transmis aux seconds et troisièmes moyens de traitement. Le générateur pseudo-aléatoire consiste en la réunion du premier générateur pseudo-aléatoire et des moyens de calcul permettant d'appliquer un algorithme de hachage aux valeurs fournies par le premier générateur pseudo-aléatoire.

De préférence selon l'invention, le système comprend un premier générateur pseudo-aléatoire pouvant être initialisé à l'aide de la clé d'initialisation. Le système comprend en outre

des septièmes moyens de traitement permettant de construire à partir de tout ou partie de la clé primaire de cryptage une suite de nombres appelée ci-après clé secondaire de cryptage. Le procédé comprend en outre des moyens de calcul permettant d'appliquer un algorithme de cryptage, utilisant comme clé de cryptage la clé secondaire de cryptage, l'algorithme de cryptage est appliqué aux valeurs fournies par le premier générateur pseudo-aléatoire. Les résultats de l'algorithme de cryptage sont transmis aux seconds et troisièmes moyens de traitement. Le générateur pseudo-aléatoire consiste en la réunion du premier générateur pseudo-aléatoire et des moyens de calcul permettant d'appliquer un algorithme de cryptage aux valeurs fournies par le premier générateur pseudo-aléatoire.

#### **Description détaillée de l'invention**

La présente invention concerne un système de cryptage dans lequel le texte crypté utilise le même jeu de symboles que le message en clair, tout en évitant les effets parasites indésirables provoqués par certaines valeurs particulières. Le texte crypté aura par construction la même longueur que le texte en clair.

Avant mise en œuvre de l'invention, on sépare en deux parties le jeu de symboles utilisé.

La première partie, ci-après appelée alphabet de contrôle, se compose des caractères de contrôle c'est-à-dire de symboles tels que sauts de lignes, retours chariot, fin de message, et plus généralement de tous les symboles qui peuvent provoquer, de la part des divers serveurs et autres dispositifs de traitement par lesquels transitent les courriers électroniques sur Internet, un comportement autre que la simple transmission du symbole. Les caractères de contrôle seront transmis en clair.

La seconde partie, ci-après appelée alphabet de message, se compose de tous les autres symboles. Ce sont ces symboles qui représentent le message proprement dit.

Le procédé et le système de cryptage, objets de la présente invention, mettent en œuvre un générateur pseudo-aléatoire. Ce générateur pseudo-aléatoire fournit des valeurs comprises dans un ensemble de valeurs ci-après dénommé espace  
5 des valeurs aléatoires. La suite des valeurs successivement fournies par le générateur pseudo-aléatoire sera ci-après dénommée séquence aléatoire.

Le générateur pseudo-aléatoire est initialisé au moyen d'une suite de nombres appelée clé d'initialisation. La séquence  
10 aléatoire fournie par le générateur pseudo-aléatoire dépend de la clé d'initialisation et après chaque initialisation utilisant la même clé d'initialisation, on obtient la même séquence aléatoire.

Lors de la mise en œuvre du procédé de cryptage et du  
15 système de cryptage, on utilise une clé de cryptage, appelée ci-après clé primaire de cryptage, la connaissance de cette clé primaire de cryptage devant ultérieurement permettre de décrypter le message qui avait été crypté avec cette clé. La clé d'initialisation est déterminée à partir de la clé de cryptage.  
20 L'utilisation de la même clé primaire de cryptage lors du décryptage assure donc que la séquence aléatoire utilisée lors du décryptage sera la même que celle utilisée lors du cryptage.

Tous les éléments de l'espace des valeurs aléatoires ne sont pas utilisables lors du cryptage. On définira un sous-  
25 ensemble, comprenant tout ou partie des éléments de l'espace des valeurs aléatoires. Ce sous-ensemble sera ci-après appelé alphabet de masque, et seuls les éléments de l'alphabet de masque seront utilisés lors du cryptage et du décryptage. A chaque élément de l'alphabet de masque on associe une  
30 permutation particulière de l'alphabet de message, c'est-à-dire une application biunivoque de l'alphabet de message dans lui-même. Cette application sera utilisée lors du cryptage. Comme elle est biunivoque, deux symboles différents auront donc deux images différentes, permettant ainsi un décryptage sans  
35 ambiguïté. Lors du décryptage, on utilisera l'application

réci-proque c'est-à-dire la permutation inverse de la permutation de celle utilisée lors du cryptage.

Une réalisation particulière de l'invention objet du présent brevet correspond à un choix particulier des permuta-tions associées aux éléments de l'alphabet de masque. Sur le plan mathématique, une réalisation particulière de l'invention correspond donc à une application de l'alphabet de masque à valeurs dans l'ensemble des permutations de l'alphabet de message.

Le nombre de choix possibles est très élevé. Si l'alphabet de message se compose de  $N$  éléments, il y a  $N!$  permutations différentes de l'alphabet de message (où  $N!$  représente le produit des  $N$  premiers entiers). Ce nombre augmente extrêmement rapidement avec  $N$ . Par exemple, pour  $N=128$ ,  $N!$  est un nombre à 215 chiffres en notation décimale classique.

De façon plus détaillée, l'opération de cryptage est réalisée comme suit. On commence par initialiser le générateur pseudo-aléatoire à l'aide de la clé d'initialisation. On lit ensuite séquentiellement, symbole par symbole, l'information à crypter. Si le symbole rencontré appartient à l'alphabet de contrôle, il n'est pas modifié. S'il appartient à l'alphabet de message, on lit l'élément suivant fourni par le générateur pseudo-aléatoire. Si cet élément ainsi lu n'appartient pas à l'alphabet de masque, on lira l'élément suivant fourni par le générateur pseudo-aléatoire, et, si besoin, on réitérera cette opération, ce jusqu'à obtenir un élément de l'alphabet de masque, appelé ci-après élément de masque. On utilisera la permutation de l'alphabet de message associée à cet élément de masque. Cette permutation est, en tant qu'application de l'alphabet de message à valeurs dans lui-même, appliquée au symbole à crypter, le résultat venant prendre la place du symbole à crypter. On réitère ces opérations pour chacun des symboles composant l'information à crypter. La suite des



éléments de masques générés lors de ces opérations s'appelle le masque de cryptage.

L'opération de décryptage se fait de façon exactement similaire en utilisant, pour chaque symbole, non pas la permutation associée à l'élément de masque, mais la permutation inverse de cette dernière. La réinitialisation, avant décryptage, du générateur pseudo-aléatoire à l'aide de la même clé d'initialisation que lors du cryptage assure que le masque de cryptage utilisé lors du décryptage sera le même que celui utilisé lors du cryptage.

Donnons maintenant, à titre illustratif et nullement limitatif des possibilités de l'invention, quelques exemples de mise en œuvre de cette invention. Le nombre  $N$  désignant comme précédemment le nombre de symboles contenus dans l'alphabet de message, on choisit, une fois pour toutes, une numérotation de l'alphabet de message, c'est-à-dire une fonction  $f$  qui à un symbole  $x$  de l'alphabet de message associe un nombre  $f(x)$  compris entre 0 et  $N-1$ , et ce de façon biunivoque. Cette fonction sera appelée ci-après fonction de numérotation. D'un point de vue mathématique la fonction de numérotation est une bijection entre l'alphabet de message et l'ensemble des entiers modulo  $N$ . On appellera  $f^{-1}$  la fonction inverse de la fonction de numérotation, c'est-à-dire la fonction, qui à un nombre  $y$  compris entre 0 et  $N-1$  associe un symbole  $x$  de l'alphabet de message tel que  $f(x)$  soit égal à  $y$ .

Explicitons ici, à titre illustratif et nullement limitatif des possibilités de l'invention, un cas particulier d'une telle fonction  $f$  dans un exemple où le codage des symboles se fait en ASCII sur 8 bits, c'est-à-dire sur un octet, représenté par un nombre compris entre 0 et 255, et dans lequel les caractères de contrôle sont les trois octets  $x00$ ,  $x0A$  et  $x0D$  représentés par les nombres 0, 10 et 13. Dans cet exemple, le nombre  $N$  de symboles contenus dans l'alphabet de message est égal à 253. Le calcul de la fonction de numérotation  $f$  s'effectue comme suit. Étant donné un octet représentant un

élément donné de l'alphabet de message, on considère le nombre  $x$  compris entre 0 et 255 qui le représente. On applique alors successivement les trois opérations ci-après, la fonction Dec étant l'opération consistant à décrémenter un entier d'une

5 unité :

Dec( $x$ )

IF  $x > 12$  THEN Dec( $x$ )

IF  $x > 8$  THEN Dec( $x$ )

Après application de ces trois opérations, le nombre  $x$

10 a une valeur comprise entre 0 et 252 et est le nombre associé par la fonction de numérotation  $f$  à l'élément donné de l'alphabet de message.

Dans le présent exemple, les valeurs fournies par le générateur pseudo-aléatoire seront des nombres et l'alphabet de

15 masque aura même taille que l'alphabet de message et se composera de l'ensemble des nombres compris entre 0 et 252. Pour définir précisément le système de cryptage utilisé, il faudra choisir 253 permutations particulières de l'alphabet de masque parmi les factorielle (253), qui est un nombre à 500 chiffres en

20 notation décimale, permutations possibles. Le nombre de possibilités est donc gigantesque.

Donnons maintenant, à titre illustratif et nullement limitatif des possibilités de l'invention, un choix particulier de permutation de l'alphabet de message. Nous faisons ici le

25 choix d'associer à un élément  $m$  de l'alphabet de masque la permutation, c'est-à-dire l'application biunivoque, qui à un nombre  $x$  compris entre 0 et 252 associe le reste par 253 de la somme  $x+m$ . Les permutations choisies correspondent donc à des additions en arithmétique modulo 253. Les permutations inverses

30 correspondent bien évidemment à des soustractions modulo 253.

De façon très détaillée, l'algorithme de cryptage consiste, une fois initialisé le générateur pseudo-aléatoire à l'aide de la clé d'initialisation, à sélectionner l'un après l'autre les symboles composant ladite information à crypter, et

à crypter chacun des symboles ainsi sélectionnés en lui appliquant les opérations suivantes :

si ledit symbole sélectionné appartient à l'alphabet de contrôle, il n'est pas modifié,

5 si ledit symbole sélectionné appartient à l'alphabet de message on lui applique les opérations (a) à (g) suivantes :

(a) on applique, au code ASCII (nombres compris entre 0 et 255) dudit symbole sélectionné, la fonction de numérotation  $f$  définie préalablement, ce qui fournit un nombre  $x$  compris  
10 entre 0 et 252.

-----  
(b) on lit le prochain nombre fourni par ledit générateur pseudo-aléatoire ,

(c) si le nombre lu à l'étape précédente est supérieur à 252, on réitère l'opération précédente jusqu'à obtention d'un  
15 nombre inférieur ou égal à 252, qui sera, ci-après, noté  $m$ .

(d) on effectue l'addition  $y = x + m$

(e) si  $y$  est supérieur à 252, on lui retranche 253

(f) le nombre  $y$  a maintenant une valeur comprise entre 0 et 252, et on lui applique la fonction  $f^{-1}$  , fonction inverse  
20 de la fonction de numérotation, qui fournit le symbole  $z$  de l'alphabet de message tel que  $f(z)$  soit égal à  $y$ .

(g) ce symbole  $z$  remplacera ledit symbole sélectionné de ladite information à crypter.

Ces opérations étant exécutées, on passe au symbole  
25 suivant de l'information à crypter, et ainsi de suite jusqu'à ce que tous les symboles de l'information à crypter aient été traités ;

Le décryptage se fait de façon similaire après nouvelle initialisation du générateur pseudo-aléatoire à l'aide  
30 de la clé d'initialisation, les opérations (d) et (e) étant remplacées par les opérations (d') et (e') ci-après

(d') on effectue la soustraction  $y = x - m$

(e') si  $y$  est négatif, on lui ajoute 253

L'une des idées originales de l'invention, dans cet  
35 exemple particulier, consiste à utiliser les masques non pas

avec un opérateur XOR mais avec une addition dans l'ensemble des entiers modulo 253. Mais il fallait avoir eu au préalable l'idée de séparer le jeu de caractères en deux parties pour se débarrasser des caractères de contrôle, puis l'idée de ramener,  
 5 par la bijection  $f$ , l'alphabet de message à l'ensemble des entiers modulo  $N$  (avec ici  $N=253$ ). L'innovation résulte, dans cette réalisation particulière, de la juxtaposition de ces trois idées. Notons que l'idée de l'addition modulo  $N$  avec les éléments d'un masque est en substance dans les travaux de  
 10 Vigenère, lire par exemple Blaise de Vigenère, Traicté des chiffres, ou secretes manieres d'escrire, paru en 1586, bien qu'au XVII<sup>ème</sup> siècle on ignorât tout de l'arithmétique modulaire.

L'utilisation d'une addition modulaire ou d'une  
 15 soustraction modulaire, détaillée dans cet exemple particulier, est un cas particulier simple de réalisation de l'invention objet du présent brevet. Il a été présenté ici en arithmétique modulo  $N$  avec  $N = 253$ , mais il peut être réalisé de façon similaire pour toute valeur raisonnable de  $N$ , en adaptant  
 20 l'algorithme de calcul de la fonction de numérotation  $f$ .

L'addition et la soustraction peuvent être remplacées par d'autres permutations de l'alphabet de message.

On peut par exemple utiliser la multiplication modulaire. Les opérations (d) et (e) sont alors remplacées par  
 25 le calcul du produit  $x.m$  (où on note par un point « . » l'opération de multiplication), puis du reste par  $N$  du résultat de cette multiplication. Mais pour que l'opération ainsi réalisée soit une bijection, il faut que le nombre  $m$  soit premier à  $N$ . Il faut donc, dans l'étape (c), non seulement  
 30 refuser les nombres supérieurs à  $N$ , mais aussi les nombres qui ne sont pas premiers à  $N$ .

L'opération réciproque de la multiplication par  $m$  modulo  $N$  est la division par  $m$  modulo  $N$ , qui, elle-aussi, nécessite que le nombre  $m$  soit premier à  $N$ . Connaissant le  
 35 nombre  $x$ , il s'agira, à l'étape (d) de trouver un nombre  $y$  tel

que le produit  $y.m$  diffère de  $x$  d'un multiple entier de  $N$ . Il faut donc en pratique trouver deux entiers  $y$  et  $z$  tels que  $y.m + N.z = x$ . Le théorème de Bezout permet de prouver qu'il y a une solution, pour toutes les valeurs possibles de  $x$ , dès que  $m$  est premier à  $N$ . A l'étape (e), on calculera le reste par  $N$  de ce nombre  $y$ .

On peut aussi utiliser l'exponentiation modulaire, les opérations (d) et (e) étant ici remplacées par le calcul du reste par  $N$  de l'élévation de  $x$  à la puissance  $m$ . Cette exponentiation modulaire est une bijection, et admet donc une réciproque, lorsque le nombre  $N$  n'a pas de facteurs carrés et que l'exposant  $m$  est un nombre non nul premier à  $\Phi(N)$ , où  $\Phi(N)$  représente le nombre d'entiers compris entre 1 et  $N-1$  et premiers à  $N$ .

L'opération réciproque est l'extraction de racine  $m$ -ième en arithmétique modulo  $N$ , c'est-à-dire le calcul du reste par  $N$  d'un nombre  $y$  qui, élevé à la puissance  $m$ , modulo  $N$ , redonne un nombre qui diffère de  $x$  d'un multiple entier de  $N$ . On peut démontrer que cette opération est équivalente à une élévation de  $x$  à une puissance  $p$ , modulo  $N$ , où  $p$  est tel que l'expression  $m.p-1$  soit un multiple entier de  $\Phi(N)$ . On peut trouver un nombre  $p$ , vérifiant cette condition, dès que  $m$  est non nul et premier à  $\Phi(N)$ .

Dans les exemples ci-dessus, il est possible de retrouver la valeur de l'élément de masque  $m$ , modulo  $N$  ou modulo  $\Phi(N)$  selon le cas, par la simple donnée du symbole en clair et du symbole crypté. Plus précisément, la donnée du message en clair et du message crypté permet de déterminer le masque, donc donne des indications très fortes sur la séquence aléatoire fournie par le générateur pseudo-aléatoire. Le nombre d'éléments de l'alphabet de masque est proche du nombre d'éléments de l'alphabet de message.

On peut mettre en œuvre l'invention en choisissant des permutations plus sophistiquées conçues de façon que la connaissance d'un symbole en clair et en crypté ne permette pas

de déterminer précisément l'élément de masque utilisé. Un exemple peut être fourni par des fonctions homographiques. On se place dans le cas où le nombre  $N$  d'éléments de l'alphabet de message est un nombre premier et on choisit un alphabet de masque significativement plus grand que l'alphabet de message. L'idéal serait que le nombre d'éléments de l'alphabet de masque soit de l'ordre de grandeur du cube du nombre  $N$  d'éléments de l'alphabet de message, ou même plus grand. On choisit alors, pour chaque élément de l'alphabet de masque, quatre nombres notés  $p$ ,  $q$ ,  $r$  et  $s$  compris entre 0 et  $N-1$  et tels que d'une part le nombre  $r$  et d'autre part le résultat de l'expression  $p.s - q.r$  soient tous deux non nuls et non multiples de  $N$ . Ces quatre nombres sont alors les 4 paramètres d'une fonction homographique en arithmétique modulaire, fonction qui remplacera celle mise en œuvre à l'étape (d) des exemples précédents. Cette fonction est la transposition en arithmétique modulaire de la fonction qui, en arithmétique classique sur les nombres réels s'écrit  $y = (p.x + q) / (r.x + s)$  et a pour graphe une hyperbole d'asymptotes parallèles aux axes de coordonnées. En arithmétique classique, toutes les valeurs de  $y$  sont atteintes une et une seule fois sauf  $y = p/r$  (qui correspond à l'ordonnée de l'asymptote horizontale) et la fonction n'est pas définie pour  $x = -s/r$ , qui correspond à l'abscisse de l'asymptote verticale. Pour que la fonction devienne une bijection, on conviendra de donner à la fonction la valeur  $p/r$  lorsque la variable  $x$  vaut  $-s/r$ . Pour transposer le calcul de cette fonction en arithmétique modulo  $N$ , on calcule dans un premier temps le dénominateur c'est-à-dire l'expression  $r.x + s$ . Si le résultat de ce calcul est nul ou est un multiple de  $N$ , la valeur  $y$  prise par la fonction est une valeur comprise entre 0 et  $N-1$  et telle que l'expression  $r.y - p$  soit un multiple, éventuellement nul, de  $N$ . Dans le cas contraire la valeur  $y$  prise par la fonction est une valeur comprise entre 0 et  $N-1$  et telle que l'expression  $(r.x + s).y - (p.x + q)$  soit un multiple, éventuellement nul, de  $N$ . La fonction réciproque de cette fonction homographique est elle-

même une fonction homographique dont les paramètres sont faciles à calculer.

On peut développer des procédés et des systèmes de cryptage selon la présente invention en utilisant des familles  
 5 de permutations bien plus riches que dans les exemples illustratifs présentés précédemment. On peut par exemple associer à certains éléments de l'alphabet de masque des additions modulaires, à d'autres des multiplications modulaires, à d'autres encore, des permutations bien plus complexes. Plus  
 10 ces permutations seront complexes, plus sera difficile la tâche d'un éventuel pirate désirant attaquer le système, mais le gain en sécurité apporté par une plus grande complexité des permutations se paiera en terme de temps de calcul nécessaire au cryptage et au décryptage de l'information.

La technique de cryptage présentée ci-dessus a l'inconvénient suivant : la connaissance simultanée du texte en clair et du texte à chiffrer permet d'obtenir des indications sur le masque. Dans le cas où on utilise une addition, une soustraction, une multiplication ou une division en arithmétique  
 20 modulaire, il suffit de connaître un symbole en clair et le même symbole crypté pour déterminer immédiatement l'élément de masque qui a servi à crypter ce symbole. C'est à peine plus difficile dans le cas de l'exponentiation modulaire ou de l'extraction de racine. L'utilisation de fonctions plus sophistiquées comme la  
 25 fonction homographique, ne permettent plus de déterminer de façon précise le masque mais elles donnent néanmoins des indications susceptibles d'être utiles à un pirate qui souhaiterait attaquer le système. Ce peut être rédhibitoire lorsqu'on utilise un générateur pseudo-aléatoire de faible  
 30 qualité, dans lequel la connaissance des aléas précédemment tirés est susceptible de fournir des informations sur les tirages futurs. Une telle attaque est appelée attaque par prédiction sur le générateur pseudo-aléatoire. Certains générateurs pseudo-aléatoires évitent cet inconvénient. Il en est  
 35 ainsi des générateurs basés sur un algorithme de chiffrement par

blocs utilisé en mode rétroaction de sortie, dit OFB pour « Output-feedback », tels que décrits page 216 et suivantes de la seconde édition de « Cryptographie Appliquée » de Bruce Schneier, - International Thomson Publishing France, 1997. Il en  
 5 de même pour le procédé décrit dans la demande de brevet déposée à l'INPI le 12 septembre 2001 sous le numéro FR0111776 et publiée le 14 mars 2003 sous le numéro FR 2829643.

Lorsque le générateur pseudo-aléatoire ne paraît pas suffisamment protégé contre les attaques par prédiction, on peut  
 10 introduire une étape intermédiaire consistant à effectuer divers traitements sur les aléas issus du générateur aléatoire en vue d'obtenir des masques dont la connaissance ne permet pas d'obtenir des informations utiles sur les aléas qui ont permis de les générer. Une technique possible est de soumettre les  
 15 aléas issus du générateur aléatoire à un algorithme de hachage à sens unique, voir par exemple « Cryptographie Appliquée » de Bruce Schneier, déjà cité, chapitres 2.3, 2.4 et 18, les empreintes fournies par ce hachage servant ensuite à générer les masques. Une autre technique possible consiste à utiliser un  
 20 algorithme de cryptage qui s'appliquera aux aléas issus du générateur aléatoire et dont les résultats serviront à générer les masques. La clé de cryptage utilisée pour cette génération de masque pourra être calculée à partir de la clé primaire de cryptage définie précédemment.

#### 25        **Description des figures**

La figure 1 présente le schéma général de l'invention.

La figure 2 illustre le cas particulier où le générateur pseudo-aléatoire GA consiste en la réunion d'un premier générateur pseudo-aléatoire et d'un système mettant en  
 30 œuvre un algorithme de hachage.

La figure 3 illustre le cas particulier où le générateur pseudo-aléatoire GA consiste en la réunion d'un premier générateur pseudo-aléatoire et d'un système mettant en œuvre un algorithme de cryptage.



Sur la figure 1, la clé primaire de cryptage CP est utilisée par les premiers moyens de traitement TR1 pour générer la clé d'initialisation CI. Cette clé d'initialisation CI sert alors à initialiser le générateur pseudo-aléatoire GA qui  
 5 fournit la séquence SA dont les éléments seront par la suite pris en compte séquentiellement. Seuls les éléments de SA qui appartiennent à l'alphabet de masque seront utilisés pour le cryptage et le décryptage. Les seconds moyens de traitement TR2 permettent de vérifier si un élément de SA appartient à  
 10 l'alphabet de masque, et les troisièmes moyens de traitement lisent les valeurs successives de la séquence aléatoire SA, jusqu'à obtenir un élément M reconnu par TR2 comme appartenant à l'alphabet de masque. Cet élément M sera appelé masque M et sera transmis aux cinquièmes moyens de traitement TR5.

15 Les symboles S composant l'information I à crypter ou à décrypter sont lus par le moyen d'une unité d'entrée sortie UES, et transmis aux quatrièmes moyens de traitement TR4 qui permettent de décider quels sont les symboles S à transmettre sans modification et quels sont les symboles S à crypter ou à  
 20 décrypter.

Étant donné un symbole S, reconnu par TR4 comme étant à crypter ou à décrypter, et le masque M fourni par TR3, les cinquièmes moyens de traitement TR5 calculent la permutation de l'alphabet de message déterminée par M ou l'inverse de cette  
 25 permutation, selon qu'on désire crypter ou décrypter, et l'appliquent au symbole S pour fournir comme résultat un symbole R qui sera transmis par une unité d'entrée sortie UES et qui destiné à remplacer le symbole S dans l'information I à crypter ou à décrypter.

30 Dans le cas où la permutation utilisée est une fonction homographique, des sixièmes moyens de traitement TR6 sont mis en œuvre pour déterminer les paramètres de la fonction homographique associée au masque M.

Sur la figure 2, le générateur pseudo-aléatoire GA se  
 35 compose d'un premier générateur pseudo-aléatoire GA1 initialisé

par la clé d'initialisation CI elle-même calculée par les moyens de traitements TR1 à partir de la clé primaire de cryptage CP. Les moyens de calcul H appliquent un algorithme de hachage aux valeurs fournies par GA1, et ce sont les résultats de cet algorithme de hachage qui forment la séquence aléatoire SA. Le générateur pseudo-aléatoire GA apparaît donc comme la réunion de GA1 et de H.

Sur la figure 3, le générateur pseudo-aléatoire GA se compose d'un premier générateur pseudo-aléatoire GA1 initialisé par la clé d'initialisation CI elle-même calculée par les moyens de traitements TR1 à partir de la clé primaire de cryptage CP. Les moyens de calcul K appliquent un algorithme de cryptage aux valeurs fournies par GA1, et ce sont les résultats de cet algorithme de hachage qui forme la séquence aléatoire SA. L'algorithme de cryptage utilise comme clé de cryptage la clé secondaire CS qui est calculée à partir de la clé primaire CP à l'aide des septièmes moyens de traitement TR7. Le générateur pseudo-aléatoire GA apparaît ici comme la réunion de GA1 et de K.

20

REVENDICATIONS

1. Procédé pour le cryptage et le décryptage d'une information (I) ; ladite information (I) étant représentée par une suite de symboles (S) ; lesdits symboles (S) étant pris dans un ensemble de symboles appelé ci-après l'alphabet ; ledit
- 5 procédé étant caractérisé en ce qu'il met en œuvre un générateur pseudo-aléatoire (GA) fournissant une séquence de valeurs dénommée ci-après séquence aléatoire (SA), les valeurs formant ladite séquence aléatoire (SA) étant incluses dans un ensemble
- ~~ci-après dénommé l'espace des valeurs aléatoires ;~~
- 10 ledit générateur pseudo-aléatoire (GA) pouvant être, avant utilisation et fourniture de ladite séquence aléatoire (SA), initialisé au moyen d'une suite de nombres ci-après dénommée clé d'initialisation (CI) ; ladite clé d'initialisation (CI) déterminant la séquence aléatoire (SA) qui sera fournie par
- 15 ledit générateur pseudo-aléatoire (GA),
- de telle sorte qu'après une initialisation ultérieure utilisant la même clé d'initialisation la séquence de valeurs fournies sera la même qu'après la première initialisation ;
- ledit générateur pseudo-aléatoire étant en outre
- 20 caractérisé en ce que la connaissance de ladite séquence des valeurs fournies ne permet pas de retrouver en un temps raisonnable ladite clé d'initialisation ;
- ledit procédé comprenant trois étapes préalables :
- l'étape préalable de séparer en deux parties
- 25 disjointes ledit alphabet, l'une desdites parties étant ci-après dénommée l'alphabet de contrôle et étant composée de symboles destinés à ne pas être modifiés lors du cryptage, l'autre desdites parties étant ci-après dénommée l'alphabet de message et étant composée de symboles destinés à être éventuellement
- 30 modifiés lors du cryptage,
- de sorte que chacun des symboles utilisés pour représenter l'information est inclus, soit dans ledit alphabet

de contrôle, soit dans ledit alphabet de message, aucun symbole n'étant commun à ces deux alphabets,

- l'étape préalable de définir un ensemble, appelé alphabet de masque, formé de tout ou partie des éléments de l'espace des valeurs aléatoires,

- l'étape préalable d'affecter à chaque élément dudit alphabet de masque une permutation dudit alphabet de message ;

lesdites trois étapes préalables étant réalisées une fois pour toutes avant la première mise en œuvre dudit procédé ;

la mise en œuvre dudit procédé, pour réaliser l'opération de cryptage d'une information (I) à crypter, comprenant les étapes préliminaires suivantes :

- l'étape de prendre en compte une suite de nombres ci-après dénommée la clé primaire de cryptage (CP),

- l'étape de construire ladite clé d'initialisation (CI) à partir de tout ou partie de ladite clé primaire de cryptage (CP) ;

- l'étape d'initialiser ledit générateur pseudo-aléatoire (GA) à l'aide de ladite clé d'initialisation (CI) ;

ledit procédé consistant à sélectionner l'un après l'autre les symboles (S) composant ladite information (I) à crypter, et à crypter chacun des symboles (S) ainsi sélectionnés en lui appliquant les opérations suivantes :

si ledit symbole (S) sélectionné appartient à l'alphabet de contrôle, il n'est pas modifié,

si ledit symbole (S) sélectionné appartient à l'alphabet de message les étapes suivantes sont exécutées :

- l'étape de lire la prochaine valeur de la séquence aléatoire (SA) fournie par ledit générateur pseudo-aléatoire (GA),

- si la valeur lue à l'étape précédente n'est pas un élément dudit alphabet de masque, l'étape de réitérer l'étape précédente jusqu'à obtention d'un élément dudit alphabet de masque,

l'élément dudit alphabet de masque, déterminé à l'étape précédente, sera ci-après dénommé l'élément de masque (M),

5 - l'étape de sélectionner la permutation de l'alphabet de message affectée audit élément de masque (M) spécifié à l'étape précédente,

- l'étape d'appliquer audit symbole (S) sélectionné la permutation de l'alphabet de message sélectionnée à l'étape précédente,

10 - l'étape de remplacer ledit symbole (S) sélectionné par le résultat (R) de la permutation mise en œuvre à l'étape précédente,

ces opérations étant exécutées, on passe au symbole (S) suivant de l'information (I) à crypter, et ainsi de suite  
15 jusqu'à ce que tous les symboles de l'information (I) à crypter aient été traités.

2. Procédé selon la revendication 1 ; la mise en œuvre dudit procédé, pour réaliser l'opération de décryptage d'une information (I) à décrypter, comprenant les mêmes étapes  
20 préliminaires que lors du cryptage,

de sorte que le générateur pseudo-aléatoire sera initialisé de la même façon que lors du cryptage et fournira donc la même séquence de valeurs que lors du cryptage ;

25 ledit procédé consistant à sélectionner l'un après l'autre les symboles (S) composant ladite information (I) à décrypter, et à décrypter chacun des symboles (S) ainsi sélectionnés en lui appliquant les opérations suivantes :

si ledit symbole (S) sélectionné appartient à l'alphabet de contrôle, il n'est pas modifié,

30 si ledit symbole (S) sélectionné appartient à l'alphabet de message les étapes suivantes sont exécutées :

- l'étape de lire la prochaine valeur de la séquence aléatoire (SA) fournie par ledit générateur pseudo-aléatoire (GA),

- si la valeur lue à l'étape précédente n'est pas un élément dudit alphabet de masque, l'étape de réitérer l'étape précédente jusqu'à obtention d'un élément dudit alphabet de masque,

5 l'élément dudit alphabet de masque, déterminé à l'étape précédente, sera ci-après dénommé l'élément de masque (M),

- l'étape de sélectionner la permutation inverse de la permutation de l'alphabet de message affectée audit élément  
10 de masque (M) spécifié à l'étape précédente,

- l'étape d'appliquer au symbole (S) sélectionné la permutation inverse sélectionnée à l'étape précédente,

- l'étape de remplacer le symbole (S) sélectionné par le résultat (R) de la permutation mise en œuvre à l'étape  
15 précédente,

ces opérations étant exécutées, on passe au symbole (S) suivant de l'information (I) à décrypter, et ainsi de suite jusqu'à ce que tous les symboles de l'information à décrypter aient été traités.

20 3. Procédé selon la revendication 1 ou 2 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, de sorte que l'alphabet de masque se compose de nombres ;

ledit procédé comprenant en outre une opération  
25 préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message, de  
30 sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole de l'alphabet de message dont ce nombre soit le numéro ;

ledit procédé étant caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément  
35 de masque (M) donné, pour un symbole (S) donné appartenant à

l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro dudit symbole (S) donné,
  - 5           - l'étape d'ajouter ledit élément de masque (M) donné au numéro déterminé à l'étape précédente,
  - l'étape de calculer le reste de la division par N du résultat de l'addition effectuée à l'étape précédente,
  - l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente, ce symbole est alors le résultat (R) que l'on
- 
- souhaitait calculer,

de sorte que la permutation ainsi définie correspond à une addition modulo N sur les numéros de symboles, et que le

15   symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée audit symbole donné.

4. Procédé selon la revendication 1 ou 2 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, de sorte que l'alphabet de masque se compose de

20   nombres ;

ledit procédé comprenant en outre une opération préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre

25   compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message,

de sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole dont ce nombre soit le numéro ;

ledit procédé étant caractérisé en ce que le résultat

30   de la permutation de l'alphabet de message associée à un élément de masque (M) donné, pour un symbole (S) donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro dudit symbole (S) donné,
- 35   donné,

- l'étape de soustraire ledit élément de masque (M) donné au numéro déterminé à l'étape précédente,
- lorsque le résultat de la soustraction effectuée à l'étape précédente est négatif, l'étape d'ajouter à ce résultat 5 autant de fois que nécessaire le nombre N jusqu'à obtenir un nombre positif,
- l'étape de calculer le reste de la division par N du résultat de l'étape précédente,
- l'étape de déterminer le symbole de l'alphabet de 10 message dont le numéro est le nombre calculé à l'étape précédente, ce symbole est alors le résultat (R) que l'on souhaitait calculer,

de sorte que la permutation ainsi définie correspond à une soustraction modulo N sur les numéros de symboles, et que le 15 symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée audit symbole donné.

5. Procédé selon la revendication 1 ou 2 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, de sorte que l'alphabet de masque se compose de 20 nombres ;

ledit procédé comprenant en outre une opération préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre 25 compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message,

de sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole dont ce nombre soit le numéro ;

ledit alphabet de masque ne comprenant que des nombres 30 non nuls et premiers à N ; ledit procédé étant caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque (M) donné, pour un symbole (S) donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :



- l'étape de déterminer le numéro dudit symbole (S) donné,
  - l'étape de multiplier par l'élément de masque (M) donné le numéro déterminé à l'étape précédente,
  - 5       - l'étape de calculer le reste de la division par N du résultat de la multiplication effectuée à l'étape précédente,
  - l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente. Ce symbole est alors le résultat (R) que l'on
  - 10       souhaitait calculer,
- 
- de sorte que la permutation ainsi définie correspond à une multiplication modulo N sur les numéros de symboles, et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée audit symbole donné.
- 15       6. Procédé selon la revendication 1 ou 2 ; les valeurs dudit espace des valeurs aléatoires étant des nombres,
  - de sorte que l'alphabet de masque se compose de nombres ;
  - ledit procédé comprenant en outre une opération
  - 20       préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message,
  - 25       de sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole dont ce nombre soit le numéro ;
  - ledit alphabet de masque ne comprenant que des nombres non nuls et premiers à N ; ledit procédé étant caractérisé en ce que le résultat de la permutation de l'alphabet de message
  - 30       associée à un élément de masque (M) donné, pour un symbole (S) donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :
  - l'étape de déterminer le numéro dudit symbole (S) donné,

- l'étape de déterminer un nombre qui, multiplié par l'élément de masque (M) donné, diffère du numéro déterminé à l'étape précédente, d'un multiple entier de N,

5 - l'étape de calculer le reste de la division par N du nombre déterminé à l'étape précédente,

- l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente. Ce symbole est alors le résultat (R) que l'on souhaitait calculer,

10 de sorte que la permutation ainsi définie correspond à une division modulo N sur les numéros de symboles, et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée audit symbole donné.

15 7. Procédé selon la revendication 1 ou 2 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, de sorte que l'alphabet de masque se compose de nombres ;

ledit procédé comprenant en outre une opération préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message

20 de sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole dont ce nombre soit le numéro ;

ledit alphabet de masque ne comprenant que des nombres non nuls et premiers à  $\Phi(N)$  où  $\Phi(N)$  désigne le nombre d'entiers compris entre 1 et N-1 et premiers à N ; ledit procédé étant caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque (M) donné, pour un symbole (S) donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes

30 suivantes :  
- l'étape de déterminer le numéro dudit symbole (S) donné,  
35

- l'étape de calculer le reste de la division par N du résultat de l'élévation du numéro déterminé à l'étape précédente à une puissance égale à l'élément de masque (M) donné,

5                   - l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente. Ce symbole est alors le résultat (R) que l'on souhaitait calculer,

de sorte que la permutation ainsi définie correspond à  
10 une exponentiation modulaire sur les numéros de symboles, et que  
le symbole déterminé à l'étape précédente est alors le résultat  
de cette permutation appliquée audit symbole donné.

8. Procédé selon la revendication 1 ou 2 ; les valeurs dudit espace des valeurs aléatoires étant des nombres,  
15 de sorte que l'alphabet de masque se compose de nombres ;

ledit procédé comprenant en outre une opération préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque symbole de  
20 l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et N-1, ci-après dénommé numéro du symbole, N représentant le nombre d'éléments de l'alphabet de message,

de sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole dont ce nombre soit le numéro ;  
25                   ledit alphabet de masque ne comprenant que des nombres non nuls et premiers à  $\Phi(N)$  où  $\Phi(N)$  désigne le nombre d'entiers compris entre 1 et N-1 et premiers à N ; ledit procédé étant caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque (M) donné,  
30 pour un symbole (S) donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le numéro dudit symbole (S) donné,

- l'étape de déterminer un nombre positif, qui, élevé à une puissance égale à l'élément de masque (M) donné, diffère du numéro déterminé à l'étape précédente d'un multiple entier de N,

5                   - l'étape de déterminer le reste de la division par N du nombre déterminé à l'étape précédente,

                  - l'étape de déterminer le symbole de l'alphabet de message dont le numéro est le nombre calculé à l'étape précédente. Ce symbole est alors le résultat (R) que l'on  
10                   souhaitait calculer,

                  de sorte que la permutation ainsi définie correspond à l'extraction d'une racine en arithmétique modulaire sur les numéros de symboles, et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée  
15                   audit symbole donné.

                  9. Procédé selon la revendication 1 ou 2 ; ledit procédé comprenant une opération préalable consistant à associer à chaque élément de l'alphabet de masque un quadruplet de nombres notés p, q, r et s et tels que le nombre r et le  
20                   résultat de l'expression  $p.s-q.r$  soient tous deux des nombres non nuls et non multiples de N, N représentant le nombre d'éléments de l'alphabet de message ; ledit procédé comprenant en outre une opération préalable de numérotation de l'alphabet de message, ladite numérotation consistant à attribuer à chaque  
25                   symbole de l'alphabet de message, sans omission ni répétition, un nombre compris entre 0 et N-1, ci-après dénommé numéro du symbole,

                  de sorte que pour tout nombre compris entre 0 et N-1 il y ait un et un seul symbole dont ce nombre soit le numéro ;

30                   ledit procédé étant caractérisé en ce que le résultat de la permutation de l'alphabet de message associée à un élément de masque (M) donné, pour un symbole (S) donné appartenant à l'alphabet de message, peut être calculé en exécutant successivement les étapes suivantes :

- l'étape de déterminer le quadruplet de nombres  $p$ ,  $q$ ,  $r$  et  $s$  associé à l'élément de masque (M) donné,
- l'étape de déterminer le numéro du symbole (S) à crypter ou à décrypter, ce numéro étant ci-après noté  $m$ ,
- 5       - l'étape de calculer l'expression  $m.r + s$ ,
- l'étape, lorsque le résultat du calcul effectué à l'étape précédente est nul ou est un multiple de  $N$ , de calculer un nombre  $k$  tel que l'expression  $k.r - p$  soit un multiple de  $N$ ,
- 10       - l'étape, lorsque le résultat du calcul effectué à l'étape précédente n'est ni zéro ni un multiple de  $N$ , de calculer un nombre positif  $k$  tel que l'expression  $k.(m.r + s) - (m.p + q)$  soit un multiple de  $N$ ,
- l'étape de calculer le reste de la division par  $N$
- 15       du nombre  $k$  calculé à l'étape précédente,
- l'étape de déterminer le symbole de l'alphabet de masque dont le numéro est le nombre calculé à l'étape précédente. Ce symbole est alors le résultat (R) que l'on souhaitait calculer,
- 20       de sorte que la permutation ainsi définie correspond au calcul d'une fonction homographique en arithmétique modulaire sur les numéros de symboles, et que le symbole déterminé à l'étape précédente est alors le résultat de cette permutation appliquée audit symbole donné.
- 25       **10.** Procédé selon l'une quelconque des revendications 1 à 9 ; ledit procédé mettant en œuvre un premier générateur pseudo-aléatoire (GA1) pouvant être initialisé à l'aide de ladite clé d'initialisation (CI) ;
- les valeurs fournies par ledit premier générateur pseudo-aléatoire étant utilisées comme données en entrée d'un
- 30       algorithme de hachage dont les résultats sont utilisés pour fournir ladite séquence aléatoire (SA) ;
- ledit générateur pseudo-aléatoire (GA) consistant en la composition dudit premier générateur pseudo-aléatoire (GA1)
- 35       et dudit algorithme de hachage.

11. Procédé selon l'une quelconque des revendications 1 à 9 ; ledit procédé comprenant en outre l'étape préliminaire de construire à partir de tout ou partie de ladite clé primaire de cryptage (CP) une suite de nombres appelée ci-après clé  
5 secondaire de cryptage (CS) ;

ledit procédé mettant en œuvre un premier générateur pseudo-aléatoire (GA1) pouvant être initialisé à l'aide de ladite clé d'initialisation (CI), les valeurs fournies par ledit premier générateur pseudo-aléatoire (GA1) étant cryptées à  
10 l'aide d'un premier algorithme de cryptage utilisant comme clé de cryptage ladite clé secondaire de cryptage (CS), les résultats dudit premier algorithme de cryptage étant utilisés pour fournir ladite séquence aléatoire (SA) ;

ledit générateur pseudo-aléatoire (GA) consistant en  
15 la composition dudit premier générateur pseudo-aléatoire (GA1) et dudit premier algorithme de cryptage.

12. Système pour le cryptage et le décryptage d'une information (I) ; ladite information (I) étant représentée par une suite de symboles (S) ; lesdits symboles (S) étant pris dans  
20 un ensemble de symboles appelé ci-après l'alphabet ; ledit alphabet étant séparé en deux parties disjointes, l'une desdites parties étant ci-après dénommée l'alphabet de contrôle et étant composée de symboles destinés à ne pas être modifiés lors du cryptage, l'autre desdites parties étant ci-après dénommée  
25 l'alphabet de message et étant composée de symboles destinés à être éventuellement modifiés lors du cryptage ;

ledit système étant plus particulièrement destiné à sécuriser les communications entre un ordinateur ci-après dénommé l'ordinateur client et un réseau formé d'un ou plusieurs  
30 autres ordinateurs, ledit système étant intercalé entre ledit ordinateur client et ledit réseau,

de sorte que toute information circulant entre ledit ordinateur client et ledit réseau et devant être cryptée ou décryptée, passe à travers ledit système ;

ledit système comprenant un générateur pseudo-aléatoire (GA) fournissant une séquence de valeurs dénommée ci-après séquence aléatoire (SA), les valeurs formant ladite séquence aléatoire (SA) étant comprises dans un ensemble ci-après dénommé l'espace des valeurs aléatoires ; certaines de ces valeurs étant incluses dans un sous-ensemble dudit espace des valeurs aléatoires, sous-ensemble ci-après dénommé alphabet de masque ;

ledit générateur pseudo-aléatoire (GA) pouvant être, avant utilisation et fourniture de ladite séquence de valeurs, initialisé au moyen d'une suite de nombres ci-après dénommée clé d'initialisation (CI) ; ladite clé d'initialisation (CI) déterminant la séquence aléatoire (SA) qui sera fournie par le générateur ;

ledit système comprenant en outre :

- deux unités d'entrée sortie (UES), l'une d'entre elles étant destinée à assurer les communications entre ledit système et ledit ordinateur client, l'autre d'entre elles étant destinée à assurer les communications entre ledit système et ledit réseau ;

- des premiers moyens de traitement (TR1) permettant de prendre en compte une suite de nombres ci-après dénommée la clé primaire de cryptage (CP), et de construire ladite clé d'initialisation (CI) à partir de tout ou partie de ladite clé primaire de cryptage (CP),

- des seconds moyens de traitement (TR2) permettant de décider si une valeur appartenant audit espace de valeurs aléatoires appartient audit alphabet de masque,

- des troisièmes moyens de traitement (TR3) permettant de lire les valeurs successives fournies par ledit générateur pseudo-aléatoire, jusqu'à obtenir un élément (M) appartenant audit alphabet de masque,

- des quatrièmes moyens de traitement (TR4) permettant de décider, parmi les symboles (S) transitant à travers ledit système, quels sont les symboles qui doivent être

cryptés ou décryptés et quels sont les symboles qui doivent être transmis sans modification,

- des cinquièmes moyens de traitement (TR5) permettant d'une part, à partir d'un élément donné de l'alphabet de masque, ci-après appelé l'élément de masque (M), de sélectionner une permutation de l'alphabet de message, cette permutation étant ci-après appelée permutation affectée à l'élément de masque (M), et permettant d'autre part, la permutation affectée à l'élément de masque (M) étant ainsi sélectionnée, et un élément donné de l'alphabet de message (S) étant fourni par l'une des deux dites unités d'entrée sortie, de déterminer le résultat (R) de cette permutation appliquée audit élément donné (S) fourni, et d'envoyer sur l'autre des deux dites unités d'entrée sortie le résultat (R) ainsi déterminé.

13. Système selon la revendication 12 ; lesdits cinquièmes moyens de traitement (TR5) permettant en outre de sélectionner la permutation inverse de ladite permutation affectée à un élément (M) de l'alphabet de masque.

14. Système selon la revendication 12 ou 13 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, lesdits cinquièmes moyens de traitement (TR5) permettant en outre d'associer un nombre à un symbole (S) dudit alphabet de message, de faire une addition en arithmétique modulaire entre ledit nombre et un élément (M) dudit alphabet de masque, et d'associer au résultat de cette addition un élément (R) de l'alphabet de message.

15. Système selon la revendication 12 ou 13 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, lesdits cinquièmes moyens de traitement (TR5) permettant en outre d'associer un nombre à un symbole (S) dudit alphabet de message, de faire une soustraction en arithmétique modulaire entre ledit nombre et un élément (M) dudit alphabet de masque, et d'associer au résultat de cette soustraction un élément (R) de l'alphabet de message.



16. Système selon la revendication 12 ou 13 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, lesdits cinquièmes moyens de traitement (TR5) permettant en outre d'associer un nombre à un symbole (S) dudit alphabet de message, de faire une multiplication en arithmétique modulaire entre ledit nombre et un élément (M) dudit alphabet de masque, et d'associer au résultat de cette multiplication un élément (R) de l'alphabet de message.

17. Système selon la revendication 12 ou 13 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, lesdits cinquièmes moyens de traitement (TR5) permettant en outre d'associer un nombre à un symbole (S) dudit alphabet de message, de faire une division en arithmétique modulaire entre ledit nombre et un élément (M) dudit alphabet de masque, et d'associer au résultat de cette division un élément (R) de l'alphabet de message.

18. Système selon la revendication 12 ou 13 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, lesdits cinquièmes moyens de traitement (TR5) permettant en outre d'associer un nombre à un symbole (S) dudit alphabet de message, de faire une exponentiation en arithmétique modulaire dudit nombre avec pour exposant un élément (M) dudit alphabet de masque, et d'associer au résultat de cette exponentiation un élément (R) de l'alphabet de message.

19. Système selon la revendication 12 ou 13 ; les valeurs dudit espace des valeurs aléatoires étant des nombres, lesdits cinquièmes moyens de traitement (TR5) permettant en outre d'associer un nombre à un symbole (S) dudit alphabet de message, de faire une extraction de racine en arithmétique modulaire, et d'associer au résultat de cette extraction de racine un élément (R) de l'alphabet de message.

20. Système selon la revendication 12 ou 13 ; le nombre de symboles composant ledit alphabet de message étant ci-après dénommé N, ledit système comportant en outre des sixièmes moyens de traitement (TR6) permettant d'associer à un élément

(M) dudit alphabet de masque un quadruplet de nombres notés p, q, r et s, lesdits cinquièmes moyens de traitement (TR5) permettant en outre :

- d'associer à un symbole dudit alphabet de message, un nombre compris entre 0 et N-1, ce nombre étant ci-après noté m,
- de calculer l'expression  $m.r + s$ ,
- de déterminer si une expression est nulle ou multiple de N,
- de calculer un nombre k compris entre 0 et N-1 et tel que l'expression  $k.r - p$  soit un multiple de N,
- de calculer un nombre k compris entre 0 et N-1 et tel que l'expression  $k.(m.r + s) - (m.p + q)$  soit un multiple de N,
- d'associer à un nombre k ainsi calculé un élément (R) de l'alphabet de message.

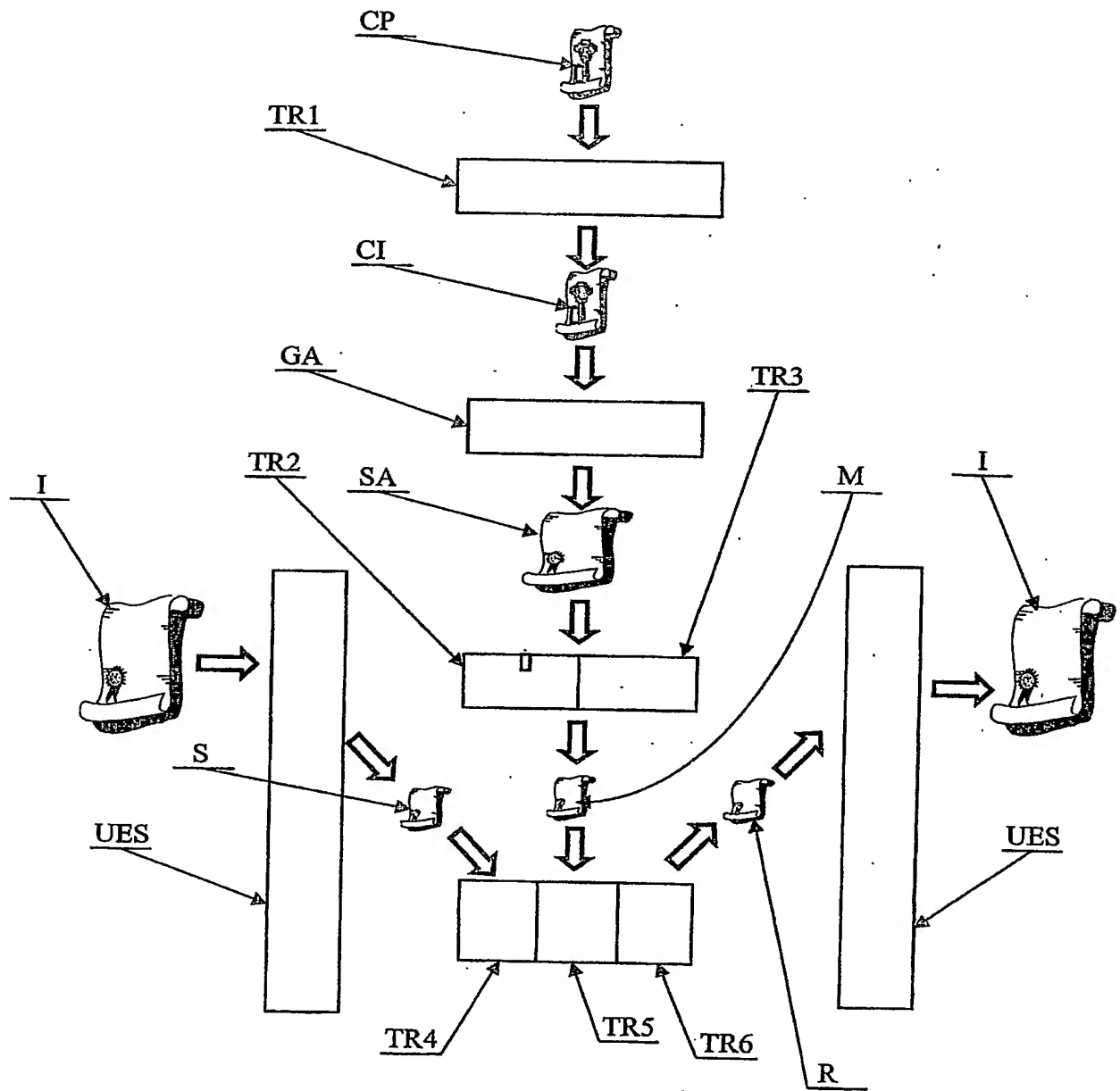
21. Système selon l'une quelconque des revendications 12 à 20 ; ledit système comprenant un premier générateur pseudo-aléatoire (GA1) pouvant être initialisé à l'aide de ladite clé d'initialisation (CI) et des moyens de calcul (H) permettant d'appliquer un algorithme de hachage aux valeurs fournies par ledit premier générateur pseudo-aléatoire (GA1), les résultats dudit algorithme de hachage étant transmis auxdits seconds et troisièmes moyens de traitement (TR2, TR3), ledit générateur pseudo-aléatoire (GA) consistant en la réunion dudit premier générateur pseudo-aléatoire (GA1) et desdits moyens de calcul (H) permettant d'appliquer un algorithme de hachage aux valeurs fournies par ledit premier générateur pseudo-aléatoire (GA1).

22. Système selon l'une quelconque des revendications 12 à 20 ; ledit système comprenant un premier générateur pseudo-aléatoire (GA1) pouvant être initialisé à l'aide de ladite clé d'initialisation (CI) ; ledit système comprenant en outre des septièmes moyens de traitement (TR7) permettant de construire à partir de tout ou partie de ladite clé primaire de cryptage (CP) une suite de nombres appelée ci-après clé secondaire de cryptage

(CS) ; ledit procédé comprenant en outre des moyens de calcul (K) permettant d'appliquer un algorithme de cryptage, utilisant comme clé de cryptage ladite clé secondaire de cryptage (CS), ledit algorithme de cryptage étant appliqué aux valeurs fournies  
5 par ledit premier générateur pseudo-aléatoire (GA1), les résultats dudit algorithme de cryptage étant transmis auxdits seconds et troisièmes moyens de traitement (TR2 , TR3), ledit générateur pseudo-aléatoire (GA) consistant en la réunion dudit premier générateur pseudo-aléatoire (GA1) et desdits moyens de  
10 calcul (K) permettant d'appliquer un algorithme de cryptage aux valeurs fournies par ledit premier générateur pseudo-aléatoire (GA1).

---

FIGURE 1



FIG\_1

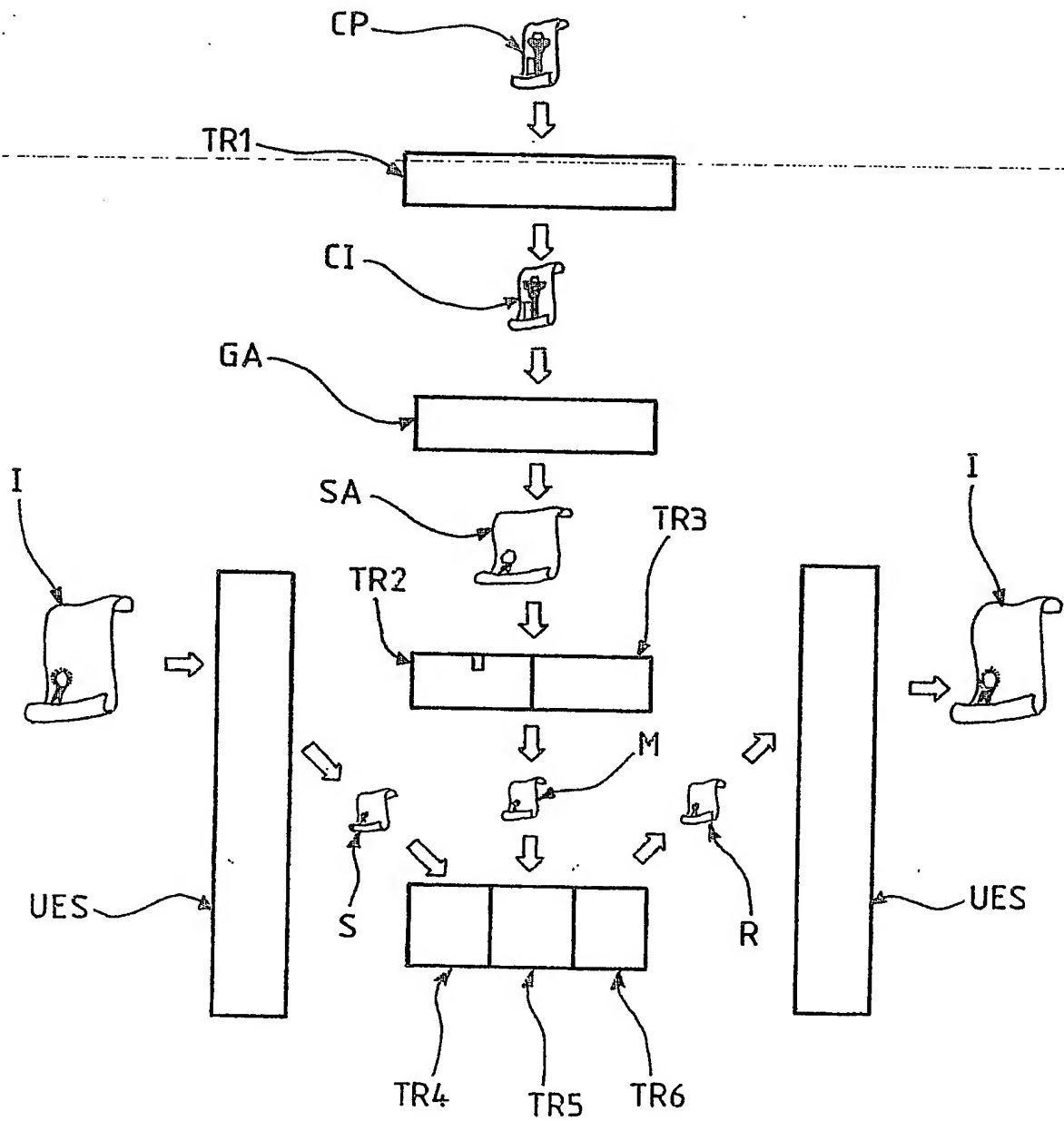
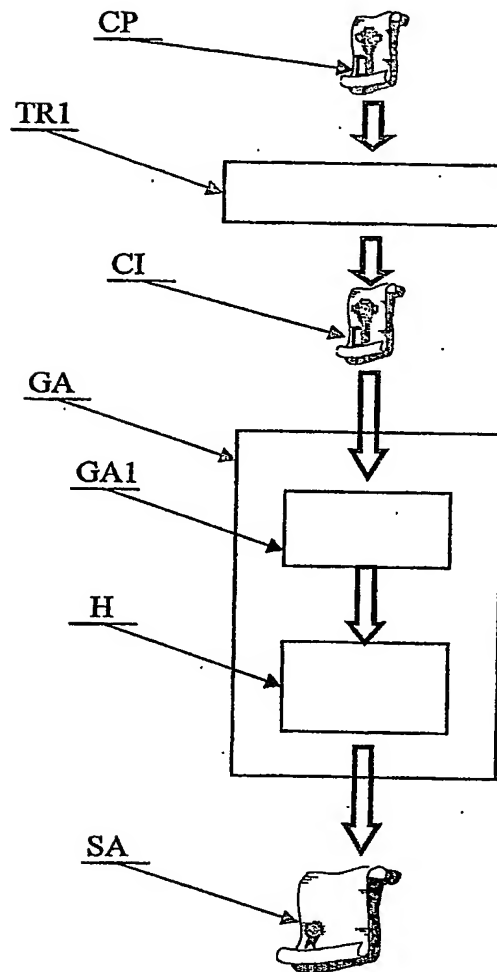


FIGURE 2



FIG\_2

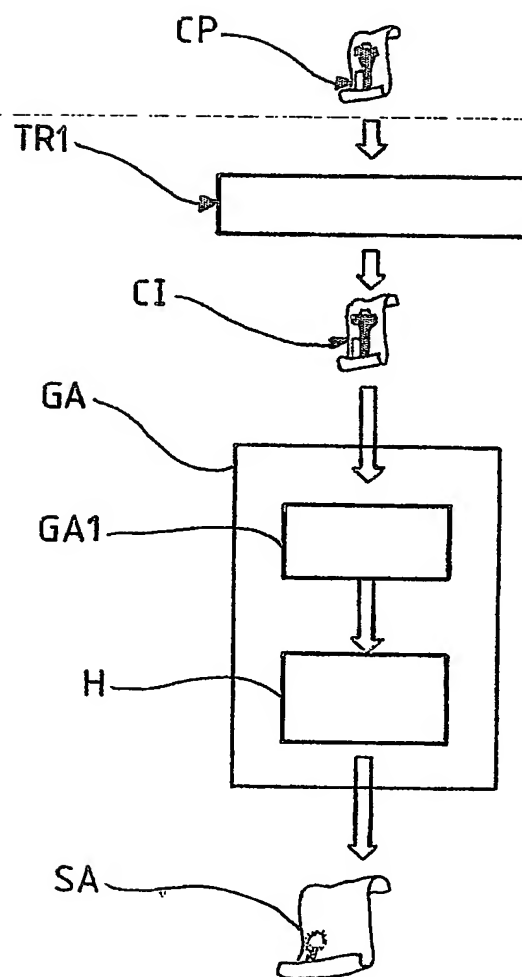


FIGURE 3

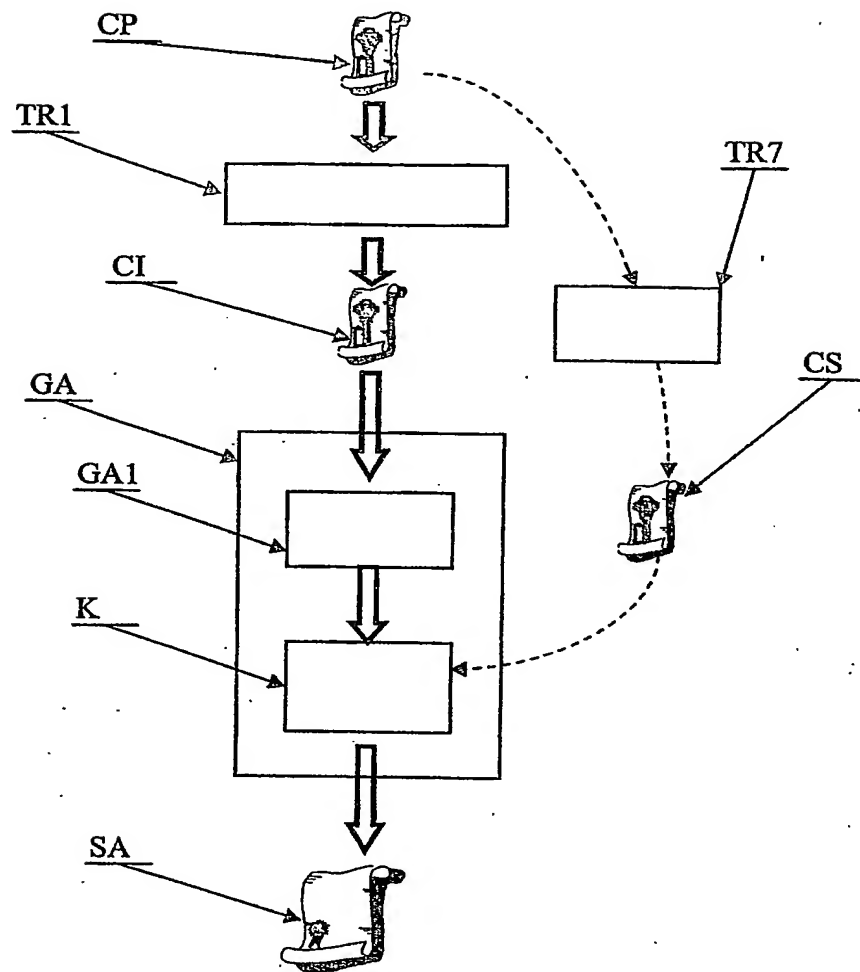
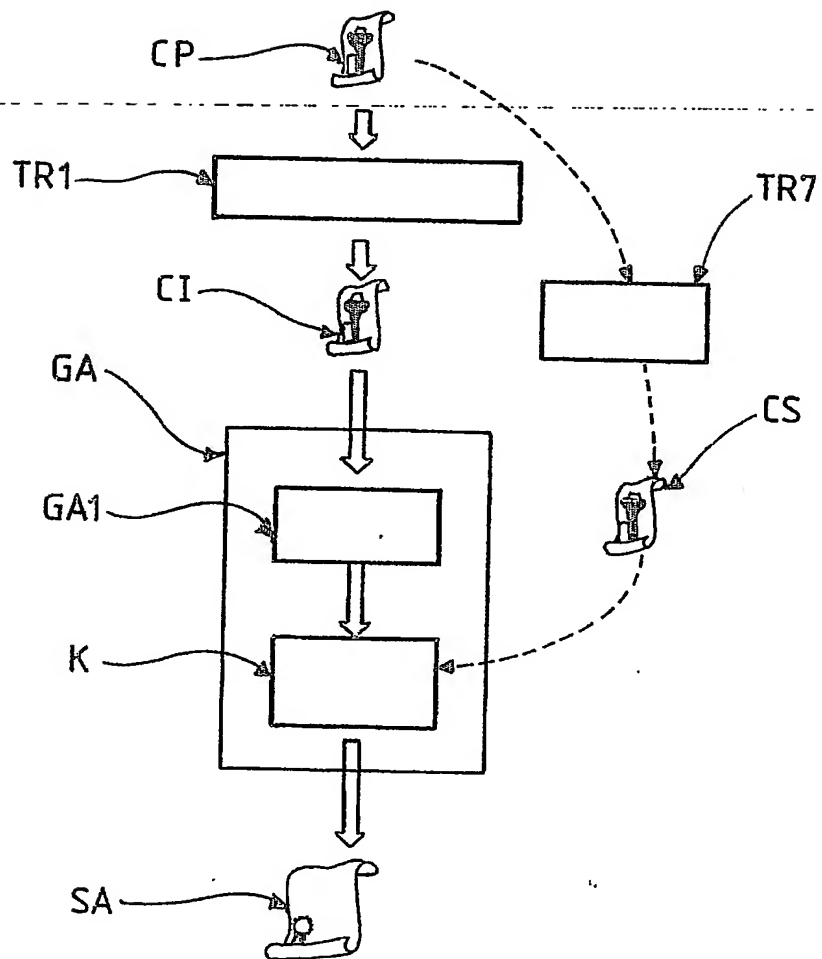
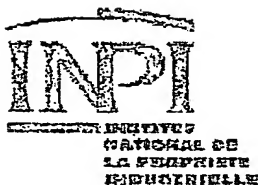




FIG. 3




# BREVET D'INVENTION

## Désignation de l'inventeur

Vos références pour ce dossier	B11023
N° D'ENREGISTREMENT NATIONAL	0303846
TITRE DE L'INVENTION	
	PROCEDE ET SYSTEME DE CRYPTAGE
LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):	

DESIGNE(NT) EN TANT QU'INVENTEUR(S):	
Inventeur 1	
Nom	STEHLÉ
Prénoms	Jean-luc
Rue	300, rue de Vaugirard
Code postal et ville	75002 PARIS
Société d'appartenance	

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE	
Signé par:	
	
Date	28 mars 2003

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PCT/FR2004/050127



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**